Enterprise Security & Data Boundary Brief

Zero PII Gateway · Z3 Pre-Commit Prover · Full 256-Bit SHA-256 WORM Ledger

01 Zero Trust Control Architecture

1. Bijective SYM_* Gateway (Mode B)

Replaces IBANs, tax numbers, and credentials in RAM before cloud LLM dispatch. Unproxied webhooks sit outside gateway scope.

2. Offline Sovereign Mode (Mode A)

Runs inside customer bare metal or VPC with local Qwen2.5-Coder / DeepSeek vLLM and local Z3 5.4.1 with zero outbound internet.

3. Firecracker / Seccomp Sandbox

Untrusted scripts execute with cap_drop: ALL, read-only rootfs, default-deny egress, and a strict 24-syscall seccomp-bpf allowlist.

4. 256-Bit WORM Audit Trail

Every gated action commits a full 256-bit SHA-256 hash chain entry + secp256r1 ECDSA signature in append-only storage.

02 Deployment Tiers, Rollback & Vendor Assurances

• Reversal Scope: Local PostgreSQL savepoint WAL undo (<25ms) & Odoo account.move.reversal (<38ms RPC) never pretend to undo external bank wires—those require human CFO sign-off.

• Zero Training on Customer Data: Customer payloads are never used to train external foundation models; federated rule distillation extracts anonymized AST invariants only.

• Compliance & Contact: Audit readiness for SOC 2 Type II and ISO/IEC 42001 in progress. Direct founder & security response: sofian@apodictic.ai | security@apodictic.ai.